Claims

What is claimed is:

Sub A1 1. A method for using a system for on-line recruitment of candidates for clinical trials comprising the step of:

receiving over a network from a computer terminal an end user's on-line consent to an electronic agreement relating to volunteering as a potential candidate for a clinical trial and the release of at least one of medical and personal information.

2. A method in accordance with claim 1, wherein the electronic agreement is a click wrap consent agreement.

Sub A2 3. A method in accordance with claim 1, further comprising generating an electronic survey form to be displayed at the computer terminal, in response to receipt of the end user's consent to the electronic agreement.

4. A method in accordance with claim 3, wherein the electronic survey form comprises at least one of personal and medical related questions.

Sub A3 5. A method in accordance with claim 3, further comprising encrypting data entered by the user in response to the survey form.

6. A method in accordance with claim 5, further comprising transmitting the encrypted data to a secure server via the network.

7. A method in accordance with claim 6, wherein the network is one of an Internet,

world wide web, intranet, local area network, wide area network, and wireless communication network.

8. A method in accordance with claim 6, further comprising decrypting the data received at said secure server.

9. A method in accordance with claim 8, further comprising storing the decrypted data in a first memory device associated with said secure server.

10. A method in accordance with claim 9, further comprising processing the decrypted data retrieved from the first memory device.

11. A method in accordance with claim 10, further comprising encrypting the processed data.

12. A method in accordance with claim 11, further comprising replacing the decrypted data in the first memory device with the encrypted processed data.

13. A method in accordance with claim 12, further comprising transmitting the encrypted processed data from said secure server to a central office.

14. A method in accordance with claim 13, further comprising storing the encrypted processed data in a second memory device associated with said central office.

15. A method in accordance with claim 14, further comprising the steps of:

in response to a request from an authorized individual, retrieving the encrypted processed data from the second memory device; and

decrypting the retrieved encrypted processed data from the second memory device.

Sub A4

16. A method in accordance with claim 1, further comprising generating a certificate to verify transmission between the end user and secure server.

17. A method in accordance with claim 3, wherein the computer terminal employs a web browser capable of supporting a secure socket layer protocol.

18. A method in accordance with claim 8, further comprising ensuring that decrypted data stored at said secure server is not accessed by unauthorized personnel.

19. A method in accordance with claim 18, wherein said ensuring step comprises at least one of limiting access to said secure server to a minimum number of authorized personnel, identifying as authorized personnel only trustworthy employees, and devising and implementing procedures to ensure that only authorized personnel gain access to the decrypted data.

Sub A5

20. A method in accordance with claim 1, further comprising generating using said secure server an electronic opt-out form to be displayed on the computer terminal to remove the end user's name from a list of volunteers as possible candidates for clinical trials.

21. A method in accordance with claim 1, wherein the electronic agreement satisfies all federal, state, and local rules, ordinances and regulations.

22. A method in accordance with claim 11, wherein said secure server encrypts the data based on a shareware encryption protocol.

23. A method in accordance with claim 27, wherein said shareware encryption protocol is Pretty Good Privacy.

24. A method in accordance with claim 15, wherein said decryption of the retrieved encrypted data from the second memory device is performed using encryption keys stored on a disk kept under physical surveillance.

Sub A6 25. A method for using a system for on-line recruitment of candidates for clinical trials comprising the step of:

providing on-line consent by an end user at a computer terminal to an electronic agreement relating to volunteering as a potential candidate for a clinical trial and release of at least one of medical and personal information.

26. A method in accordance with claim 25, wherein the electronic agreement is a click wrap consent agreement.

Sub A7 27. A method in accordance with claim 25, further comprising, after providing consent to the electronic agreement, responding at the end user's computer terminal to information solicited in an electronic survey form.

28. A method in accordance with claim 27, wherein the electronic survey form comprises at least one of personal and medical related questions.

Sub A8 29. A method in accordance with claim 27, wherein the electronic survey form is received by the user's computer terminal via a network.

30. A method in accordance with claim 29, wherein the network is one of an Internet, world wide web, Intranet, local area network, wide area network, and wireless communications network.

Sub A9 31. A system for on-line recruitment of candidates for clinical trials over a network

~~comprising:~~

~~a secure server generating an electronic agreement; and~~

~~at least one computer terminal on which is displayed the electronic agreement, said at least one computer terminal used by an end user to provide consent to said electronic agreement to volunteer as a potential candidate for a clinical trial and release at least one of medical and personal data, said secure server and said at least one computer terminal being connected via the network.~~

~~32. A system in accordance with claim 31, wherein said secure server, in response to the end user consenting to the electronic agreement, generates an electronic survey form at said at least one computer terminal.~~

33. A system in accordance with claim 32, wherein the electronic survey form comprises at least one of personal and medical related questions.

34. A system in accordance with claim 33, wherein said at least one computer terminal is used to enter at least one of personal and medical data in response to the questions in the electronic survey form.

35. A system in accordance with claim 34, wherein said at least one computer terminal includes web browser software for encrypting the response data entered at said at least one computer terminal.

36. A system in accordance with claim 35, wherein said encrypted response data is received by said secure server from said at least one computer terminal via the network.

37. A system in accordance with claim 36, wherein said secure server decrypts the encrypted response data.

38. A system in accordance with claim 37, wherein said secure server includes a first memory device for storing the decrypted response data.

39. A system in accordance with claim 38, wherein said secure server processes the decrypted response data retrieved from said first memory device.

40. A system in accordance with claim 39, wherein said secure server encrypts the processed data.

41. A system in accordance with claim 40, wherein said secure server replaces the decrypted response data in said first memory device with said encrypted processed data.

42. A system in accordance with claim 41, further comprising a central office connected to said secure server.

43. A system in accordance with claim 42, wherein said secure server and central office are a single device at the same location.

44. A system in accordance with claim 43, wherein said central office receives the encrypted processed data transmitted from said secure server.

45. A system in accordance with claim 44. wherein said central office includes a second memory device for storing the encrypted processed data.

46. A system in accordance with claim 45, wherein said central office, in response to a request from an authorized individual, retrieves and decrypts the encrypted processed data from said second memory device.

47. A system in accordance with claim 35, wherein said web browser software is capable of supporting a secure socket layer protocol.

48. A system in accordance with claim 46, wherein said secure server ensures that the decrypted processed data is not accessed by unauthorized personnel.

49. A system in accordance with claim 48, wherein said secure server ensures that the decrypted processed data is not accessed by unauthorized personnel by limiting access to said secure server to a minimum number of authorized personnel.

Sub A10 50. A system in accordance with claim 31, wherein said secure server generates an electronic opt-out form on said at least one computer terminal to remove a volunteer's name as a possible candidate for clinical trials.

51. A system in accordance with claim 31, wherein said electronic agreement satisfies all federal, state and local laws and regulations concerning dissemination of medical, health and personal information.

52. A system in accordance with claim 31, wherein said network is one of an Internet, world wide web, Intranet, local area network, wide area network, and wireless communication network.

Sub A11 53. A method in accordance with claim 1, further comprising the step of receiving an end user's section of at least one from a list of a plurality of possible clinical trials to volunteer as a potential candidate.

54. A method in accordance with claim 53, further comprising the step of permitting access of at least one of medical and personal information only by representatives of the

selected clinical trials.

ADD A12